It passes through the piercing points S and T, near L and B, of LB with the cylindrical surface. Every point of the cylinder gives rise to such a curve, so that a doubly infinite number of curves is obtained which all pass through T. In Fig. 2, three lamps at L, L', L'' at equal intervals and their corresponding curves are shown.

A number of problems suggest themselves in connection with a detailed study of these curves. As an example the result may be stated, that the locus of the foci of all conics (ellipses) cut out on the surface by the planes of the pencil through LB is a twisted quartic, whose orthogonal projection on a plane normal to LB passes through the circular points.

Referring again to Fig. 2, it is clear that the quartic through S and T is determined by ST and does not depend on the position of L and B on ST. Hence assuming on ST, L and B arbitrarily, there are generally only a limited number of points on the quartic where reflexion towards B takes place, so that geometrically there are no continuous curves of reflexion.

The reason why such curves are seen physically lies in the fact that in reality the tunnel-surface consists of rectangular plane pieces and the source of light of a luminous body. In place of an incident and reflected ray at each point of the quartic we therefore have bundles of rays striking the plane portions around each point of the curve. On account of the proximity of L and B to the surface, parts of each bundle will be reflected to B.

ON COMPOSITE NUMBERS P WHICH SATISFY THE FERMAT CONGRUENCE $a^{P-1} \equiv 1 \bmod P$.*

By R. D. CARMICHAEL, Indiana University.

Professor J. H. Jeans† has discussed the question of the converse of Fermat's theorem, showing that the relation

$$a^{P-1} \equiv 1 \bmod P, \tag{1}$$

which (by Fermat's theorem) is always true when P is a prime for any value of a which is prime to P, is for any particular value of a true for values of P which are not prime. Mr. E. B. Escott‡ has given a more direct proof of the same theorem.

The failure of the converse of Fermat's theorem has also been pointed out by Lucas§ by means of the example

* Read before the American Mathematical Society, October 28, 1911.

† *Messenger of Mathematics*, 27 (1897-8), p. 174.

‡ *Messenger of Mathematics*, New Series, No. 431 (1907), p. 175.

§ *Theorie des nombres*, I, p. 422.

$$2^{37.73-1} \equiv 1 \bmod 37.73.$$

Lucas states the true converse in this form: *If a^x-1 is divisible by P for $x=P-1$, but for no other value of x which is a divisor of $P-1$, then P is a prime number.*

A detailed study of (1) for composite P has been made by Cipolla.* Among other things he shows that for every a there exists an infinite number of composite integers P satisfying (1). Conversely, for every odd P, not a power of 3, the congruence (1) is always satisfied by some number a different from ± 1.

The object of the present note is to extend the preceding results by proving the theorem that there are values of composite P for which relation (1) is true when a is any number prime to P. A necessary and sufficient condition for this will be given and a method will be explained for obtaining the appropriate values of P. The note is an amplification of an earlier remark by the present writer.†

Let a function $\lambda(m)$, where

$$m=2^{\alpha}\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

and the numbers $p_1, p_2, \ldots, p_n$ are different odd primes, be defined in the following manner:

$$\lambda(2^{\alpha})=\phi(2^{\alpha}), \text{ if } \alpha=0, 1, 2;$$
$$\lambda(2^{\alpha})=\tfrac{1}{2}\phi(2^{\alpha}), \text{ if } \alpha>2;$$
$$\lambda(p_i^{\alpha_i})=\phi(p_i^{\alpha_i}), \text{ when } p_i \text{ is an odd prime;}$$
$$\lambda(m)=\text{least common multiple of } \lambda(2^{\alpha}), \lambda(p_1^{\alpha_1}), \ldots, \lambda(p_n^{\alpha_n}).$$

Then it is well known that for every a prime to P we have the congruence

$$a^{\lambda(P)} \equiv 1 \bmod P. \tag{2}$$

Furthermore, it has been proved‡ that $\lambda(P)$ is the least exponent such that (2) is true for every a prime to P. Hence, it follows at once that if (1) is true $\lambda(P)$ must be a factor of $P-1$. Again, if $\lambda(P)$ is a factor of $P-1$ the relation (1) is satisfied for every a prime to P. Hence the following theorem:

---

* *Annali di Matematica* (3) 9 (1903), pp. 139-160.

† *Bulletin of the American Mathematical Society*, Vol. 16 (1910), pp. 237-238.

‡ *Bulletin of the American Mathematical Society*, Vol. 16 (1910), pp. 232-238.

THEOREM I. *A necessary and sufficient condition on the integer P in order that the congruence*

$$a^{P-1} \equiv 1 \bmod P$$

shall be true for every a which is prime to P is that $P-1$ shall be divisible by $\lambda(P)$; or

$$P-1 \equiv 0 \bmod \lambda(P). \tag{3}$$

From this theorem it follows at once that P and $\lambda(P)$ are relatively prime. Hence, P does not contain a repeated prime factor; for, if so, such a prime would be a factor both of P and of $\lambda(P)$—which we have just seen to be impossible. Moreover, P cannot be a product of two prime factors; for if $P=pq$ and $p>q$, it follows from theorem I that

$$\frac{pq-1}{p-1} = \text{integer}.$$

But

$$\frac{pq-1}{p-1} = q + \frac{q-1}{p-1}.$$

Since p is greater than q the second member of the last equation is not an integer. That is, $P=pq$ does not in any case satisfy theorem I. Now, $\lambda(P)$ is even since $\lambda(m)$ is even when $m \neq 2$ and P is composite so that it is not 2. Hence (3) cannot be satisfied by an even P. Collecting these results, we have

THEOREM II. *In order that composite P shall satisfy the congruence*

$$a^{P-1} \equiv 1 \bmod P$$

for every a which is prime to P it is necessary that a shall be the product of three or more different odd prime factors.

We shall now prove the following theorem:

THEOREM III. *There are values of composite P for which the congruence*

$$a^{P-1} \equiv 1 \bmod P$$

is true when a is any integer prime to P.

We shall prove this theorem by actually finding numbers P of the form

$$P=pqr$$

which satisfy the necessary and sufficient condition of theorem I, the numbers p, q, r being primes.

Evidently, a necessary condition that $P=pqr$ shall satisfy (3) is that each of the expressions

$$\frac{pqr-1}{p-1}, \quad \frac{pqr-1}{q-1}, \quad \frac{pqr-1}{p-1}$$

shall be an integer. Subtracting from these numbers in order the integers qr, rp, pq we have the result that the remainders

$$\frac{qr-1}{p-1}, \quad \frac{pr-1}{q-1}, \quad \frac{pq-1}{r-1} \tag{4}$$

must each be an integer. We shall refer to this as condition (4).

If $p=3$ it is easy to show that there is the single number 3.11.17 which satisfies condition (4), but that this number fails to satisfy the condition in theorem I. For $p=5$ two solutions satisfying (4) and theorem I are found; namely, 5.13.17 and 5.17.29. For $p=7$ we have the four solutions

$$7.13.19, \quad 7.13.31, \quad 7.19.67, \quad 7.31.73.$$

We shall illustrate the method of finding solutions by carrying out the process in detail for the case $p=7$.

For this case the first number in (4) is

$$\frac{qr-1}{6}.$$

In order that this shall be an integer it is necessary and sufficient that both q and r shall be of the form $6n+1$ or both of the form $6n-1$. From the third number in (4) we see that

$$\frac{7q-1}{r-1}=m,$$

where m has one of the values 2, 3, ..., 6, since r is greater than q. This equation gives

$$r=\frac{7q+m-1}{m}. \tag{5}$$

Substituting this value of r in the second member of (4) we find that we must have

$$\frac{4pq+6m-7}{m(q-1)}=\text{integer}=\frac{1}{m}\left(49+\frac{6m+42}{q-1}\right).$$

The values of q which satisfy this relation are the following:

For $m=2$, $q=19$;
For $m=3$, $q=13, 31$;
For $m=4$, $q=23$;
For $m=5$, $q=13, 73$;
For $m=6$, No value of q.

If we substitute in (5) and remember that r must be prime we see that $q=23$ and $q=73$ are both impossible. The other values of q in order give the numbers

$$7.19.67,\quad 7.13.31,\quad 7.31.73,\quad 7.13.19$$

as the only possible values of P which are of the form $7qr$. Testing these values by means of theorem I, we see that each of them is a possible value of P as was stated above.

In a similar way we may assume other values of p and determine all possible values of P having such a prime factor p and having the desired property of satisfying (1) for every a prime to P. The modification of the method which is necessary for dealing with P as the product of four or more different odd primes is obvious. In this way one determines the following integers P^* having the property that the congruence

* This list might be indefinitely extended.

$$a^{P-1} \equiv 1 \bmod P$$

is true for every a which is prime to P:

5.13.17	13.37.241
5.17.29	13.37.97
7.13.19	13.37.61
7.13.31	31.61.271
7.19.67	31.61.211
7.31.73	31.61.631
13.61.397	37.73.109

13.37.73.457

ON REMARKABLE POINTS OF CURVES.

By S. LEFSCHETZ, University of Nebraska.

Among the points that we define below as *remarkable*, the only ones that have been considered to any serious extent, are the well known singular points of algebraic curves. Plücker* in solving the famous Poncelet pardox on the class of the reciprocal of an algebraic curve, gave the formula connecting their numbers. Caily† subsequently gave analogous ones for twisted curves, and Veronese‡ extended his results for n-space. In what follows an attempt is made to make precise the notion of remarkable point of a curve, by defining a class of points that can be reasonably so called, and two very simple propositions concerning these points are established. It is proper to remark that the discussion is not restricted to algebraic curves.

Let us consider in a plane an innumerable aggregate A of points, and the innumerable aggregate B of lines obtained by joining any two points of the aggregate A.

* *Algebraische Kurven.*

† *Coll. Math. Papers*, Vol. 1, p. 207.

‡ *Behandlung über die Methode des Projicirens und Schneidens, Math. Ann.* Vol. 19, p. 213.